

Federal Wireless Users' Forum Workshop

May 14–16, 2002

Crowne Plaza Philadelphia – Center City

Philadelphia, Pennsylvania

Workshop Summary

Introduction

The seventeenth workshop of the Federal Wireless Users' Forum (FWUF) was held in Philadelphia, Pennsylvania, May 14–16, 2002, at the Crowne Plaza Philadelphia – Center City. The Federal Wireless Users' Forum, National Communications System (NCS), and the Federal Wireless Policy Committee sponsor the workshops. The objectives of the FWUF are to:

- Educate Federal Government users about wireless telecommunications and issues;
- Identify wireless telecommunications needs of Federal Government users;
- Facilitate information exchange with other user groups, standards organizations, manufacturers, and service providers, to ensure that Government user wireless needs are met, and;
- Support the interoperability of emerging wireless services and equipment through increased participation in the formulation of Federal policy, participation in wireless standards development, and other appropriate activities.

Requirements and issues identified at the workshop will be drafted and input to the Federal Wireless Policy Committee, other government decision-makers, the wireless industry, and standards organizations. A total of 148 individuals from Federal, state, and local government, equipment manufacturers, and wireless service providers attended the workshop to discuss wireless services, requirements, and issues.

The main focus of this particular workshop was changes in the Federal wireless landscape in the wake of the events of September 11th. Workshop topics included a panel discussion on wireless lessons of September 11th, commercial wireless services and technologies, interoperability, wireless security, and government wireless initiatives. A dialogue session focusing on user wireless requirements and issues was held to further refine government requirements, discuss issues, and share lessons learned.

The current chairperson of the FWUF, Mary Ruhl, announced that she will step down from that position following the May workshop. In her place, three co-chairs have been named: Anna Entrichel and Tim Havighurst of the National Security Agency (NSA), and Jeng Mao of the National Telecommunications and Information Administration (NTIA). Ms. Ruhl's efforts in the continued excellence of the FWUF Workshops were recognized and the new co-chairs were introduced during this workshop.

Workshop Topics

The morning of the first day began with a keynote address by Robert West (filling in for John Tritak) of the Critical Infrastructure Assurance Office (CIAO). Mr. West discussed Critical Infrastructure Assurance and the history of Federal efforts leading to creation of the CIAO. He noted the heightened concern for communication interoperability for first responders. The Office of Homeland Security, which calls for the development of a national Homeland Security strategy, has identified support to first responders as a top priority. He noted that vertical information sharing (between Federal, state, and local) and horizontal information sharing (between fire, medical, and law enforcement) must be robust and seamless and emphasized that interoperability requires both policy and technology. Wireless communications must be fully integrated into the national Homeland Security strategy.

The morning of the first day featured panel discussion on Wireless Lessons since September 11th. Industry and government panelists discussed the impact of the attacks, solutions and future plans. The afternoon session covered presentations from industry regarding emerging commercial wireless services and technologies for emergency support, Homeland Defense, and military support.

Sessions on wireless interoperability and wireless security were features of the second day. The morning of the third day continued the wireless security session with a presentation on viruses in the wireless environment, along with updates on GSA wireless offerings, wireless regulatory issues and wireless priority service. A dialogue session on users issues and requirements and a discussion of future plans concluded the workshop.

Workshop Dialogue

The goals of the workshop were to identify common themes, issues, to identify and refine user wireless requirements, and enable dialogue with government and industry participants.

September 11th Wireless Lessons

Impact

Sprint PCS reported a national overload on mobile switching centers for the initial 24 hours following the attack, affecting the T1 and T3 links. Power problems affected SS7 connectivity and redundancy. Verizon Wireless reported up to 2 times more traffic than the busiest day ever and experienced congestion across all aspects of the network—cell sites, switch, completion to long distance and local carriers. Service providers deployed COWs (Cellular On Wheels) to replace disabled cell sites and provide increased capacity. COW placement was difficult due to the urban canyon environment of lower Manhattan. Additionally, the site was considered a crime scene, restricting access and operations. Verizon Wireless and Sprint PCS provided thousands of mobile phones to law enforcement and rescue personnel.

Karl Rauscher of Lucent reported on the efforts of the Wireless Emergency Response Team, a coordinated wireless industry group providing mutual aid support for search and rescue efforts at the World Trade Center. This group assisted in the location and

communication with trapped survivors possessing a variety of wireless devices (e.g., phone, pager, key FOB). The WERT also looked for any activity on call center list, screened false 911 calls, and coordinated with the authorities and the media.

Rick Murphy, Co-Chair of the PSWN, noted that effective communications at the Pentagon was the result of nearly 20 years of planning and preparation. The 1982 Air Florida crash into the Washington DC 14th Street bridge took place at the same time as a crippling snowstorm and Metro-rail accident. These events called attention to the need for improved interoperable LMR communications in the DC area. In response, improvements were made to increase interoperability between multiple organizations and jurisdictions. While much has been accomplished, more work remains to be done.

Panelists stressed that effective interoperable communications require foresight, planning, coordination, and cooperation. Effective interoperable communications systems require:

- Coordination and cooperation across agencies and jurisdictions,
- Commitment to developing shared technical solutions and protocols
- Training and drills to ensure smooth operations in emergency response.

The current security environment calls for increased interoperability among all levels of government.

The group agreed that training on communications equipment is essential. If a system is not used on a regular basis before an emergency, it will not be of use during an emergency. Inserting new technologies during a crisis does not work. Panelists noted a high degree of cooperation and commitment between response teams and commercial organizations. This spirit of teamwork continues.

What worked well

- Cooperation between organizations
- Pre-established coordination function of the NCC (National Coordinating Center)
- Formal Incident Command System (ICS) was a key factor supporting successful communications
- Ability to conduct rapid research
- Adapted fraud, billing, and trouble-shooting tools to quickly screen call center list and 911 calls.
- Use of test equipment, portable BTS and repeaters with antennas lowered into debris to locate survivors and communicate with rescue workers

What needs improvement

- Possible addition of emergency mode for mobile equipment with extremely low power and location beacons
- Broad language translation capabilities
- Use of text messaging to communicate with victim
- Need to have mobile resources in reserve for speedy deployment
- Set up virtual command centers at Federal, state, and local levels with pre-established conference call lines

The group noted that now more than ever, people appreciate the role of government in providing safety. Government officials are listening to the needs of national security and emergency preparedness personnel. Now is the time to make progress on wireless priority service and other government wireless requirements.

Wireless Priority Service

Gary Jones of VoiceStream reported on deployment of GSM Wireless Priority Service (WPS). VoiceStream has recently deployed WPS to the greater Washington DC and New York City area. WPS will be on a subscription basis. Five thousand handsets will be provided to Federal, state, and local National Security and Emergency Preparedness (NS/EP) workers in these two areas. The U.S. GSM community is working to develop a more fully featured WPS capability for nationwide deployment by the end of 2002 and complete WPS capabilities by the end of 2003. John Graves of the National Communications System (NCS) noted WPS service for the Salt Lake City Olympics had been provided by Globalstar and Verizon Wireless. Mr. Graves noted that while current deployment is GSM-based, WPS support on CDMA-based networks is needed. However, at the current time, WPS on CDMA has been deferred due to funding issues.

It was noted that WPS and GETS are necessary to overcome network congestion and that blockages can occur in many places across the network. The specific purpose of WPS and GETS is to provide a very high probability of call completion, compared to Plain Old Telephone Service calls during periods of extremely high congestion, such as that which occurred on September 11th. While conditions may occur which can block any call, even a GETS or WPS call, these NS/EP calling services are engineered to provide the highest probability of completion possible.

Wireless Interoperability

Rick Murphy of the Public Safety Wireless Network (PSWN) presented an update on PSWN pilots focused on testing interoperability. He emphasized that there is not just one solution, but a mix of solutions. The National Wireless Infrastructure Project and Project SAFECOM were identified as key wireless interoperability programs. These two programs are being coordinated and show great promise for vertical and horizontal interoperability. Voice over IP systems are being deployed and utilized by the State of Pennsylvania and several other organizations to address interoperability at the network layer. Several speakers noted that interoperability issues cannot be solved by technology alone; policy must be established and followed to enable interoperability.

Dr. Peter Ward reported on the Partnership for Public Warning, which is a cross agency and industry forum focused on improving the nation's public warning infrastructure and the implementation and integration of public warning technologies.

Wireless Security

Security continues to be a critical requirement across wireless services for users. Users noted the lack of security in wireless services and technologies and expressed requirements for strong encryption, authentication, data integrity, and availability. Users

need to consider the security context of wireless usage in different environments, such as personal, local, and wide area.

Security vulnerabilities of wireless LAN 802.11 were discussed, as well as the potential solutions and user considerations. Bluetooth, originally intended as a cable replacement, but now seen as a ubiquitous, low-cost, low-power wireless protocol for piconets, is seen to have a number of security flaws. Speakers emphasized the importance of proper system configuration for both WLANs and Bluetooth.

Anna Entrichel and Tim Havighurst of NSA provided updates on high assurance wireless products, such as the QSEC 800, Sectera, SecNet-11, as well as the development of a secure BlackBerry device. Refer to <http://www.securephone.net> for more details on these and other secure wireless devices. Rick Brown of the Federal Bureau of Investigation (FBI) reported on field trials of secure data access to the NCIC using different commercial and private wireless systems. The draft Department of Defense (DoD) wireless policy was presented by Carlson Wiltshire of Air Force/ILCS and generated much interest among users. This policy was coordinated and developed with input across DoD and will be distributed as a DoD directive in the fall of 2002. A PKI will be required to support classified and unclassified identification and authentication.

David Perry of Trend Micro, described computer malicious code, such as viruses, worms and Trojans, and noted the potential for malicious code attacks against mobile device applications. He described two recent cell phone viruses, the 911 DOKOMO, which shut down the 911 services in Japan, and the Timfonica virus. David prescribed an integrated multi-point strategy for protection against malicious code attacks and stressed the importance of user education.

Wireless Services and Technologies

Users expressed much interest in wireless data services and noted the growing usage of PEDs (Portable Electronic Devices). Users are using a number of different wireless systems, such as CDPD, satellite, and private systems for mobile data applications. The FBI expressed requirements for imagery for downloading mug shots from the NCIC database. Several speakers emphasized the usefulness of pilots and trials of wireless services to prove user requirements and operation.

The group discussed the benefits using of different wireless services and technologies, such as cellular, satellite, mobile data, and private radio systems. Diversity gives users availability of communications and flexibility in disaster response. Users recognized that in today's world, carrying multiple wireless devices is the "cost of doing business".

It was noted that satellite broadband services can provide a solution in remote areas where terrestrial-based communications are not available. 3G wireless shows great promise for nation-wide interoperability and improved productivity with high speed, multimedia applications.

The wireless carriers noted the industry-wide trend towards disposable mobile devices, for example, the lifetime of a cellphone has changed to 2 years. Government users noted this change must be relayed to government capital planners. Government users noted that lease plans, with fixed costs, fit better into government budget planning.

Wireless Coverage

GSA has taken the lead in assisting users in communicating their wireless coverage requirements to industry and has formed a cross-agency group to examine and pursue alternative solutions. Industry and government agencies interested in participating in this effort should contact GSA.

Workshop Conclusions

The issues listed below will be raised to the Federal Wireless Policy Committee and other government decision-making organizations.

- The tragic events of September 11th underscore the critical need for wireless communications to be available and secure for emergency response and national security. There is a heightened awareness across the country for the role of government in providing safety and from government officials on NS/EP needs. Now is the time to make progress on government users' wireless requirements.
- Effective interoperable communications require foresight, planning, coordination and cooperation across agencies and jurisdictions. Training and drills are essential to ensure smooth operations in emergency response. The current security environment calls for increased interoperability among all levels of government.
- Progress has been made on the deployment of Wireless Priority Service for the greater Washington DC area and New York City, with nation-wide deployment underway. Further support for WPS is needed to ensure service across different wireless technologies.
- Security of wireless services continues to be a critical issue for government users. Users have requirements for strong encryption, authentication, access control, data integrity and availability. Users expressed concern with the security of wireless LANs, Bluetooth, and the potential for malicious code to affect wireless devices. Users requested more education on security, vulnerabilities, risk analysis and management.
- Agencies are currently employing PEDs, WLANs, CDPD, paging, mobile data networks, private radio system, satellite, and other technologies and services to support diverse applications. Users agreed that 3G wireless systems show great promise for nation-wide interoperability and improved productivity with high-speed, multimedia applications.
- Users should consider the use of different wireless services and technologies (e.g., cellular, satellite, mobile data, private radio) to support availability of

communications and disaster response. Carrying multiple wireless devices is the “cost of doing business” in today’s world. Additionally, government financial planners should recognize that mobile devices are considered to be disposable, with a lifetime of two years.

- Wireless systems are now considered to be part of the telecommunications infrastructure and must be integrated into the national Homeland Security strategy.

The FWUF workshop continues to provide valuable opportunities for sharing information and partnering among government and industry participants. Many government and industry participants expressed support and appreciation for the workshop.

The next FWUF workshop is tentatively scheduled for October 16-18, 2002 in Las Vegas NV, co-locating with the CTIA Wireless I.T. and Internet conference. Further information will be posted on the FWUF website as it becomes available.